Cloud Procurement Terms

The following legal terms establish the minimum requirements applicable to subscriptions to cloud offerings (each referred to as the "Service") by the Massachusetts Bay Transportation Authority ("Customer"). Terms may be removed without approval if Service Provider's terms contain similar provisions that are no less protective of the MBTA than the provisions contained herein. These terms must be attached to and made part of the executed contract.

A. DEFINITIONS

Cloud offerings include the following:

"Infrastructure-as-a-Service" (IaaS) means the capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed application; and possibly limited control of select networking components (e.g., host firewalls).

"Platform-as-a-Service" (PaaS) means the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.

"Software-as-a-Service" (SaaS) means the capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin-client interface such as a Web browser (e.g., Web-based email) or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

B. SUBSCRIPTION TERMS

1. Service Provider grants to Customer a license or right to (i) access and use the Service, (ii) for SaaS, use underlying software as embodied or used in the service, and (iii) view, copy, download (if applicable), and use documentation.

2. No terms, including a standard click-through license or website terms of use or privacy policy, shall apply to Customer unless Customer has expressly agreed to such terms by including them in a signed agreement.

C. SUPPORT AND TRAINING

1. Service Provider must provide technical support via online helpdesk and toll-free phone number, at minimum during Business Hours (Monday through Friday from 8:00 a.m. to 6:00 p.m. Eastern Time), and 24x7x365 if required by Customer and requested prior to contract execution.

2. Service Provider must make training available online to users. Training must be accessible, per the Executive Office of Technology Services and Security's Web Accessibility Standards. https://www.mass.gov/guides/web-accessibility-standards

3. All support and training shall be provided at no additional cost to Customer, except for customized support and training expressly requested by Customer.

D. SERVICE LEVELS

Service Provider must provide a Service Level Agreement (SLA) that contains, at minimum, the following terms:

Emergency Maintenance

For any critical defects, Service Provide shall perform emergency maintenance within 24 hours.

Uptime; scheduled maintenance

1. SLA must include (1) specified guaranteed annual or monthly uptime percentage, at minimum 99%; and (2) definition of uptime and how it is calculated.

2. For purposes of calculating uptime percentage, scheduled maintenance may be excluded up to ten (10) hours per month, but unscheduled maintenance and any scheduled maintenance in excess of ten (10) hours must be included as downtime

3. Scheduled maintenance must occur: with at least two (2) business days' advance notice; at agreed-upon times when a minimum number of users will be using the system; and in no event during Business Hours. As provided in Section K, in no event shall the Service be unavailable to Customer for a period in excess of twenty-four (24) hours.

Defects; other SLA metrics

4. SLA must include: (1) response and resolution times for defects; (2) at least three levels of defect classifications (severe, medium, low); and (3) any other applicable performance metrics (e.g., latency, transaction time) based on industry standards.

5. While the Service Provider may initially classify defects upon detection, Customer determines final classification of defects, which shall occur no later than.

Remedies

6. SLA must include remedies for failure to meet guaranteed uptime percentage, response and resolution times, and other metrics, which may include fee reductions, credits, and extensions in service period at no cost. Such remedies shall be issued by Service Provider with no action required from Customer.

7. Repeated or consistent failures to meet SLA metrics result in (1) a refund of all fees paid by Customer for the period in which the failure occurred; (2) participation by Service Provider in a root cause analysis and corrective action plan at Customer's request; and (3) a right for Customer to terminate without penalty, refund to Customer of any subscription payments previously rendered by Customer for the time period after the effective date of termination, and without waiver of any rights upon written notice to Service Provider.

Reports

8. Service Provider will provide Customer with a written report (which may be electronic) of performance metrics, including uptime percentage and record of service support requests, classifications, and response

and resolution times, at least quarterly or as requested by Customer. Customer may independently audit the report at Customer's expense.

9. Representatives of Service Provider and Customer shall meet as often as may be reasonably requested by either party to review the performance of the Service and to discuss technical plans, financial matters, system performance, service levels, and any other matters related to this Agreement.

10. Service Provider will provide to Customer regular status reports during unscheduled downtime, at least twice per day or upon request.

11. Service Provider will provide Customer with root cause analysis within fourteen (14) days of unscheduled downtime at no additional cost. Root cause analysis will provide all relevant information required by the MBTA's Root Cause Analysis Form, included as Appendix A.

Changes to SLA

12. Service Provider may not change the SLA in any manner that adversely affects Customer or degrades the service levels applicable to Customer, without Customer's written approval.

E. UPDATES AND UPGRADES

1. Service Provider will make updates and upgrades available to Customer at no additional cost when Service Provider makes such updates and upgrades generally available to its users.

2. Unless otherwise agreed to in writing, no update, upgrade or other change to the Service may decrease the Service's functionality, adversely affect Customer's use of or access to the Service, or increase the cost of the Service to Customer.

3. Service Provider will notify Customer at least sixty (60) days in advance prior to any major update or upgrade.

4. Service Provider will notify Customer at least five (5) business days in advance prior to any minor update or upgrade, including hotfixes and installation of service packs, except in the case of an emergency such as a security breach.

F. CUSTOMER DATA

1. Customer retains full right and title to data provided by Customer and any data derived therefrom, including metadata (collectively, the "Customer Data").

2. Service Provider shall not collect, access, or use user-specific Customer Data except as strictly necessary to provide Service to Customer. No information regarding Customer's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction or at Customer's direction. This obligation shall extend beyond the term of the Agreement in perpetuity.

3. Service Provider shall not use any information collected in connection with the Agreement, including the Customer Data, for any purpose other than fulfilling its obligations under the Agreement.

4. At no time may any data or processes which either belong to Customer, or are intended for Customer's exclusive use, be copied, disclosed, or retained by Service Provider for subsequent use in any transaction that does not include Customer.

5. Customer Data must remain at all times within the continental United States. Service Provider must disclose to Customer the identity of any third-party host of Customer Data prior to the signing of this Agreement.

6. Customer may export the Customer Data at any time during the term of the Agreement or for up to three (3) months after the term (so long as the Customer Data remains in the Service Provider's possession) in an agreed-upon file format and medium. Service Provider must permit export of Customer Data on a regular and automated basis.

7. Three (3) months after the termination or expiration of the Agreement or upon Customer's earlier written request, and in any event after Customer has had an opportunity to export and recover the Customer Data, Service Provider shall at its own expense destroy and erase from all systems it directly or indirectly uses or controls all tangible or intangible forms of the Customer Data and Customer's Confidential Information, in whole or in part, and all copies thereof except such records as are required by law. To the extent that any applicable law prevents Service Provider from destroying or erasing Customer Data as described in the preceding sentence, Service Provider shall retain, in its then current state, all such Customer Data then within its right of control or possession in accordance with the confidentiality, security and other requirements of this Agreement, and perform its obligations under this section as soon as such law no longer prevents it from doing so. Service Provider shall, upon request, send a written certification to Customer certifying that it has destroyed the Customer Data and Confidential Information in compliance with this section.

G. DATA PRIVACY AND SECURITY

1. Service Provider must comply with all applicable laws related to data privacy and security.

2. Service Provider shall not access Customer user accounts, or Customer Data, except in the course of data center operations, response to service or technical issues, as required by the express terms of this Agreement, or at Customer's written request.

3. Service Provider may not share Customer Data with its parent company, other affiliate, or any other third party without Customer's express written consent.

4. Prior to contract execution, Service Provider and Customer must cooperate and hold a meeting to determine whether:

a. "Personal data," as defined in Mass. Gen. Laws c. 66A, will be stored or used in the Service. If so, then Service Provider is a "holder" of "personal data", as such terms are defined in M.G.L. c. 66A, solely to the extent that the obligations of a holder are applicable to Service Provider's delivery of services under the Agreement. The Customer remains responsible for all other obligations of a holder set forth in M.G.L. c. 66A.

b. Any sensitive or personal information will be stored or used in the Service that is subject to any law, rule or regulation providing for specific compliance obligations (e.g., M.G.L. c. 93H and 201 CMR 17.00, HIPAA, FERPA, IRS Pub. 1075). If so, then Service Provider must document in the Agreement how the Service complies with such law.

If either of the above is true, then Service Provider and Customer must review the Service specifications to determine whether the Service is appropriate for the level of sensitivity of the data to be stored or used in the Service, and how Customer and Service Provider will comply with applicable laws. Service

Provider and Customer must document the results of this discussion and attach the document to the Agreement.

5. Service Provider shall provide a secure environment for Customer Data, and any hardware and software, including servers, network and data components provided by Service Provider as part of its performance under this Agreement, in order to protect, and prevent unauthorized access to and use or modification of, the Service and Customer Data.

6. Service Provider will encrypt personal and non-public Customer Data in transit and at rest.

7. Customer Data must be partitioned from other data in such a manner that access to it will not be impacted or forfeited due to e-discovery, search and seizure or other actions by third parties obtaining or attempting to obtain Service Provider's records, information or data for reasons or activities that are not directly related to Customer's business.

8. In the event of any breach of the Service's security that adversely affects Customer Data or Service Provider's obligations with respect thereto, or any evidence that leads Service Provider to reasonably believe that such a breach is imminent, Service Provider shall immediately (and in no event more than twenty-four hours after discovering such breach) notify Customer. Service Provider shall identify the affected Customer Data and inform Customer of the actions it is taking or will take to reduce the risk of further loss to Customer. Service Provider shall provide Customer the opportunity to participate in the investigation of the breach and to exercise control over reporting the unauthorized disclosure, to the extent permitted by law.

9. In the event that personally identifiable information is compromised, Service Provider shall be responsible for providing breach notification to data owners in coordination with Customer and the Commonwealth as required by M.G.L. ch. 93H or other applicable law or Commonwealth policy.

10. Service Provider shall indemnify, defend, and hold Customer harmless from and against any and all fines, criminal or civil penalties, judgments, damages and assessments, including reasonable expenses suffered by, accrued against, charged to or recoverable from the Commonwealth, on account of the failure of Service Provider to perform its obligations pursuant to this Section.

H. WARRANTY

At minimum, Service Provider must warrant that:

1. Service Provider has acquired any and all rights, grants, assignments, conveyances, licenses, permissions and authorizations necessary for Service Provider to provide the Service to Customer;

2. The Service will perform materially as described in the Agreement;

3. Service Provider will provide to Customer commercially reasonable continuous and uninterrupted access to the Service, and will not interfere with Customer's access to and use of the Service during the term of the Agreement;

4. The Service is compatible with and will operate successfully with any environment (including web browser and operating system) specified by Service Provider in its documentation;

5. The Service will be performed in accordance with industry standards, provided however that if a conflicting specific standard is provided in this Agreement or the documentation provided by Service Provider, such specific standard will prevail;

6. Service Provider will maintain adequate and qualified staff and subcontractors to perform its obligations under this Agreement; and

7. Service Provider and its employees, subcontractors, partners and third party providers have taken all necessary and reasonable measures to ensure that all software provided under this Agreement shall be free of Trojan horses, back doors, known security vulnerabilities, malicious code, degradation, or breach of privacy or security.

I. ACCESSIBILITY

For SaaS and PaaS, Service Provider must comply with the Commonwealth's established standards for accessibility as described in a separate attachment. If such attachment is not provided, the Service Provider must request the accessibility terms from Customer. The accessibility terms provide, among other things, that Service Provider must (1) give Customer a VPAT or other results of accessibility testing prior to contract execution; (2) provide Customer with access to the Service so that Customer can conduct accessibility testing, and cooperate with Customer or third party accessibility testing of the Service; and (3) make available, both prior to and during the course of the engagement, Service Provider personnel to discuss accessibility and compliance with the Commonwealth's accessibility standards.

J. SUBCONTRACTORS

1. Before and during the term of this Agreement, Service Provider must notify Customer prior to any subcontractor providing any services, directly or indirectly, to Customer under this Agreement that materially affect the Service being provided to Customer, including: hosting; data storage; security and data integrity; payment; and disaster recovery. Customer must approve all such subcontractors identified after the effective date of the Agreement.

2. Service Provider is responsible for its subcontractors' compliance with the Agreement, and shall be fully liable for the actions and omissions of subcontractors as if such actions or omissions were performed by Service Provider.

K. DISASTER RECOVERY

1. Service Provider agrees to maintain and follow a disaster recovery plan designed to maintain Customer access to the Service, and to prevent the unintended destruction or loss of Customer Data. The disaster recovery plan shall provide for and be followed by Service Provider such that in no event shall the Service be unavailable to Customer for a period in excess of twenty-four (24) hours.

2. If Customer designates the Service as mission-critical, as determined by Customer in its sole discretion: (1) Service Provider shall review and test the disaster recovery plan regularly, at minimum twice annually; (2) Service Provider shall back up Customer Data no less than twice daily in an off-site "hardened" facility located within the continental United States; and (3) in the event of Service failure, Service Provider shall be able to restore the Service, including Customer Data, with loss of no more than twelve (12) hours of Customer Data and transactions prior to failure. For Services not designated as mission-critical, Service Provider shall provide information concerning back up of Customer Data and disaster recovery.

L. RECORDS AND AUDIT

1. Records. Service Provider shall maintain accurate, reasonably detailed records pertaining to:

(i) The substantiation of claims for payment under this Agreement, and

(ii) Service Levels, including service availability and downtime.

2. Records Retention. Service Provider shall keep such records for a minimum retention period of seven (7) years from the date of creation, and will preserve all such records for five (5) years after termination of this Agreement. No applicable records may be discarded or destroyed during the course of any litigation, claim, negotiation, audit or other inquiry involving this Agreement.

3. Audit of Records. Customer or its designated agent shall have the right, upon reasonable notice to Service Provider, to audit, review and copy, or contract with a third party to audit, any and all records collected by Service Provider pursuant to item (1) above, as well as any other Service Provider records that may reasonably relate to Customer's use of the Service, no more than twice per calendar year. Such records will be made available to Customer at no cost in a format that can be downloaded or otherwise duplicated.

M. TRANSITION ASSISTANCE

1. Service Provider shall reasonably cooperate with other parties in connection with all services to be delivered under this Agreement, including without limitation any successor provider to whom Customer Data is to be transferred in connection with termination. Service Provider shall assist Customer in exporting and extracting the Customer Data, in a format usable without the use of the Service and as agreed to by Customer, at no additional cost. Any transition services requested by Customer involving additional knowledge transfer and support may be subject to a separate transition SOW on a time and materials basis either for a fixed fee or at rates to be mutually agreed upon by the parties.

2. If Customer determines in its sole discretion that a documented transition plan is necessary, then no later than sixty (60) days prior to termination, Service Provider and Customer shall jointly create a written Transition Plan Document identifying transition services to be provided and including an SOW if applicable. Both parties shall comply with the Transition Plan Document both prior to and after termination as needed.

Signature on following page

IN WITNESS WHEREOF, the Contractor certifies under the pains and penalties of perjury that it shall comply with these MBTA Cloud Procurement Terms for any applicable Contract executed with the MBTA as certified by their authorized signatory below:

Contractor Authorized Signatory: _____

Print Name: _____
(BLOCK LETTERS)

Title: _____

Date: _____

(check one) _____ Organization _____ Individual

Full legal Organization or Individual Name:			
Doing Business As Name (If Different):			
Tax Identification Number:			
Address:			
Phone:		**Fax:**	